DOC IT Security Evaluation Checklist: Information System Security Officer (ISSO) Responsibilities

An Information System Security Officer (ISSO) is a DOC federal employee or contractor who is appointed in writing by a system owner to ensure implementation of system-level security controls and to maintain system documentation.

This checklist provides ISSOs with a self-assessment tool, and their supervisors or Contracting Officer's Technical Representatives with a performance evaluation tool, to evaluate the level of compliance with ISSO duties as established by the *DOC IT Security Program Policy and Minimum Implementation Standards* (ITSPP), Section 2.1.10, as well as the additional sections of the ITSPP cited in the second column of the checklist.

This is an assessment of (name/operating unit/office):		
	Self Assessment	**Assessment Date:**
	Third Party Evaluation	**Assessor** (name/title/org.):

Status Codes: **1** = Not Started   **2** = In Process   **3** = In Place

Performance Levels:
1 ISSO is aware of comprehensive IT security policies in place
2 ISSO is aware of comprehensive IT security policies as well as detailed procedures in place
3 ISSO is familiar with comprehensive IT security policies and detailed procedures in place and fully implements them for the system
4 ISSO is familiar with comprehensive IT security policies and detailed procedures in place, fully implements them for the system, and tests them for effectiveness
5 ISSO is familiar with, and fully implements and tests, comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

Information System Security Officer (ISSO) Responsibilities	ITSPP Section Reference*	Status	Performance Levels
1 Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e. life cycle management)	17.6.2 –gives examples of common ISSO responsibilities		
2 Assist in the determination of an appropriate level of security commensurate with the impact level	3.4.1		
3 Assist in the development and maintenance of system security plans and contingency plans for all systems under their responsibility.	4.3, 9		
4 Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.	3		
5 Participate in self-assessment of system safeguards and program elements and in certification and accreditation of the system;	6		
6 Notify the responsible IT Security Officer (ITSO) of any suspected incidents in a timely manner, and assist in the investigation of incidents, as necessary;	14.7		
7 Maintain cooperative relationship with business partners or other interconnected systems.			

---

* In addition to Section 2.1.10